UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF VIRGINIA

ALEXANDRIA DIVISION

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)	MISC NO. 10-4 10GJ3703 **ORAL ARGUMENT REQUESTED**

BRIEF OF AMICI CURIAE IN SUPPORT OF OBJECTIONS OF REAL PARTIES IN INTEREST JACOB APPELBAUM, BIRGITTA JONSDOTTIR AND ROP GONGGRIJP TO MARCH 11, 2011 ORDER DENYING MOTION TO VACATE

I. INTEREST OF AMICI

Amici curiae are Steven M. Bellovin, PhD., Matt Blaze, PhD., Jim Gettys, Susan Landau, PhD., Anthony G. Lauck, Peter G. Neuman, PhD., David P. Reed, PhD., Bruce Schneier and Barbara Simons, PhD. (collectively "Amici"). Each amicus is an expert in computer network and Internet technologies as well as the security and privacy issues unique to those technologies. An abbreviated summary of each amicus' background and honors, listed in alphabetical order, is as follows:

Steven M. Bellovin, PhD. Dr. Bellovin is a professor of computer science at Columbia University, where he does research on networks, security, and especially why the two do not get along. He joined the faculty in 2005 after many years at Bell Labs and AT&T Labs Research, where he was an AT&T Fellow. He is a member of the National Academy of Engineering and is serving on the Computer Science and Telecommunications Board of the National Academies, the Department of Homeland Security's Science and Technology Advisory Committee, and the Technical Guidelines Development Committee of the Election Assistance Commission. He is the co-author of "Firewalls and Internet Security: Repelling the Wily Hacker," and holds a number patents on cryptographic and network protocols.

Matt Blaze, PhD. Dr. Blaze's research focuses on the architecture and design of secure systems based on cryptographic techniques, analysis of secure systems against practical attack models, and on finding new cryptographic primitives and techniques. This work has led directly to several new cryptographic concepts, including: "Remotely-Keyed Encryption," which allows the use of inexpensive, low-bandwidth secure hardware to protect high-bandwidth communication and stored data; "Atomic Proxy Cryptography," which allows re-encryption by untrusted third parties; and "Master-Key Encryption," which provides a systematic way to design (and study) ciphers with built-in "back doors."

Jim Gettys. Mr. Gettys is a computer programmer at Alcatel-Lucent Bell Labs, USA. Until January 2009, he was the Vice President of Software at the One Laptop per Child project, working on the software for the OLPC XO-1. He is one of the original developers of the X Window System at MIT and worked on it again with X.Org, where he served on the board of directors. He previously served on the GNOME foundation board of directors. He worked at the World Wide Web Consortium (W3C) and is the editor of the HTTP/1.1 specification in the Internet Engineering Task Force. He also helped to establish the handhelds.org community, from which the development of Linux on handheld devices can be traced.

Susan Landau, PhD. Dr. Landau is a fellow at the Radcliffe Institute for Advanced Study, Harvard University and was previously a Distinguished Engineer at Sun Microsystems. She is the author of "Surveillance or Security? The Risks Posed by New Wiretapping Technologies" and co-author of "Privacy on the Line: The Politics of Wiretapping and Encryption."

Anthony G. Lauck. Mr. Lauck is an independent consultant residing in Warren,Vermont. Previously, he was a Corporate Consulting Engineer and the Technical Director of Networking at Digital Equipment Corporation. His group at Digital developed solutions to a number of problems associated with large computer networks, including naming, routing, congestion control and security. He has contributed to standardizing network protocols since the early 1980's, when he was part of the team that developed the Ethernet standard. He was a member of the Internet Advisory Board (IAB) and the National Science Foundation Network Technical

Advisory Group. He holds patents on local area networks, data link protocols, flow and congestion control algorithms, routing protocols, and multi-protocol networking.

Peter G. Neuman, PhD. Dr. Neumann is the Principal Scientist, SRI International Computer Science Laboratory. He also serves as the moderator of the Association for Computing Machinery (ACM) Risks Forum.

David P. Reed, PhD. Dr. Reed has had a distinguished 45-year career in computer systems engineering, as a key participant in the design and implementation of the Internet, personal computing, distributed systems, radio networking, and human centered computing environments. He is known for key early contributions to the architecture of the Internet in the 1970's. In recent years, he has contributed to several areas of public technology policy issues, including opening up the wireless spectrum, opening up the debate about Deep Packet Inspection and modification and preserving the openness of the Internet worldwide.

Bruce Schneier. Internationally renowned security technologist Bruce Schneier has authored eleven books -- including "Beyond Fear and Secrets and Lies" – as well as hundreds of articles, essays, and academic papers. His influential newsletter "Crypto-Gram," and his blog "Schneier on Security" (www.schneier.com) are read by over a quarter million people. Mr. Schneier is also the Chief Security Technology Officer of BT (formerly British Telecom).

Barbara Simons, PhD. Dr. Simons is Senator Reid's appointee to the Board of Advisors of the U.S. Election Assistance Commission. She served on the President's Export Council's Subcommittee on Encryption and on the Information Technology-Sector of the President's Council on the Year 2000 Conversion. She has testified before both the U.S. and state legislatures and at government sponsored hearings. In 2005 Simons became the first woman to receive the Distinguished Engineering Alumni Award from the College of Engineering of U.C. Berkeley. Simons was President of the Association for Computing Machinery, the nation's oldest and largest educational and scientific society for computing professionals,from July 1998 until June 2000. She is a Fellow of ACM and the American Association for the Advancement of Science, and is retired from IBM Research. She was runner-up in the first election for the North America seat on the Internet Corporation for Assigned Names and Numbers (ICANN) Board.

II. INTRODUCTION

Amici support the Objections of real parties in interest Jacob Appelbaum, Birgitta Jonsdottir, and Rop Gonggrijp (collectively "Parties") because Amici believe that when a court seeks to apply a law into an area of rapidly developing technology, it is crucially important that the court correctly and fully understand that technology. Otherwise, the court's ruling could have far-reaching and unintended harmful effects, including effects that might diminish the public's perception of the wisdom and integrity of the judiciary. In this matter, the government has sought to apply 20th Century technology and 20th Century precedents to 21st Century technology. Specifically, the government has taken the position that Internet Protocol Addresses ("IP Addresses") are directly analogous to telephone numbers and that the court should simply follow U.S. Supreme Court precedents that found a minimal expectation of privacy with respect to telephone numbers. The Parties, on the other hand, assert that IP Addresses can reveal that the Parties were located in particular private spaces at particular times and that such information entails a reasonable expectation of privacy.

In fact, IP Addresses do not identify a unique device the way a telephone number identifies a unique telephone. Instead, IP Addresses identify the network that serves as the focal point from which a network-enabled device (a computer, tablet or smartphone) accesses the Internet. When a portable device moves from an Internet connection on one network (the network connection at one's home, for example) to an Internet connection on another network (a local coffee shop), the IP Address associated with the portable device will change. A large collection of data over a lengthy period of time that includes IP Addresses, dates and times – as one might get from a heavily trafficked website such as Twitter – can readily translate into a picture of a person's movements from one location to another.

The government's acquisition of such a picture of a person's movements has serious implications for a person's expectations of privacy. Those expectations of privacy should, in turn, trigger greater judicial scrutiny of Constitutional issues that arise. Thus, from the point of view of the technology at-issue, the Parties have the stronger position than the government.

III. DISCUSSION

A. The Technology Underlying IP Addresses Implicates Expectations of Privacy that are Considerably Different from the Privacy Expectations Associated with Telephone Numbers.

IP Addresses were devised as a way for bundles of data to be routed over the Internet from one computer network to another. They are expressed as four numbers separated by three decimal points in the format of xxx.xxx.xxx.xxx, where each number is between 0 and 255, inclusive.[1] (RFC 760, DOD Standard Internet Protocol, p. 7 (January 1980). An example of an IP Address is 156.128.118.200. That number represents the IP Address for the Administrative Office of the U.S. Courts in Washington D.C. (whois.domaintools.com)

There are 4.2 billion potential IP Addresses. When first devised, 4.2 billion IP Addresses was considered to be an ample sufficiency. Recent news reports indicate that because of the explosive growth of the Internet, the 4.2 billion IP Addresses is almost depleted. (www.aolnews.com/2011/02/02/internet-running-out-of-ip-addresses).[2]

IP Addresses are geographically limited to minimize the size of the routing databases. Large blocks of potential IP Addresses have been allocated to Regional Internet Registries. For North America, the Regional Internet Registry is the American Registry of Internet Numbers (ARIN), and for Europe the Registry is Réseaux IP Européens (RIPE). There are other Registries for Asia, Africa and South America. (www.arin.net/knowledge/rirs.html).

The larger Internet Service Providers (ISPs) obtain blocks of IP Addresses from the Regional Internet Registry associated with their region. The larger ISPs will reserve some IP Addresses for their own use and will allocate a smaller bundle of IP Addresses to smaller ISPs. The large and small ISPs then provide Internet access to their users and handle many associated functions, including the further assignment of IP Addresses. (www.ripe.net/internet-coordination/press-centre/understanding-ip-addressing).

Internet traffic takes the form of bundles of data that is routed through specialized

---

[1] The use of the 256 numerals between 0 and 255 is a result of the fact that computers compute at a basic level in powers of 2. The number 256 is 2^8.

[2] A new version of the Internet Protocol, IPv6, has 2^{96} more addresses than the current version and, when implemented, will alleviate this potential problem.

computers appropriately called "routers." The routers maintain a database of IP Addresses so that the router can direct the IP Addressed bundles of data to the correct location. The bundles of data must have the source ID Address to function. (communication.howstuffworks.com/convergence/router.htm).

An ISP will activate a block of IP Addresses through a process called "announcing." Upon "announcing," a router will update its database to reflect the association between the block of IP Addresses and the destination/ISP, and then the router will communicate the new information to other routers in an automated fashion. (arstechnica.com/old/content/2008/02/-insecure-routing-redirects-youtube-to-pakistan.ars[3]).

The ISPs assign IP Addresses to the networks within the ambit of their service. Those networks, in turn, serve as points of access to the Internet for network-enabled devices, namely, computers, tablets (such as the iPad) and smartphones (such as the iPhone or Androoid-based phone). (www.opendns.com/support/article/81).

Many network-enabled devices use an automated process called the Dynamic Host Configuration Protocol (DHCP). Dial-up and (most) DSL modems use the Point-to-Point Protocol (PPP). Each of these protocols automatically exchanges information with the host network through which the device seeks an Internet connection. As a result of that exchange of information, the host network undertakes the final inward-bound routing of bundles of data from the Internet to an individual device, and the person's outward-bound activity on the Internet will reflect the IP Address of the host network that his device has joined. Because the information exchange and Internet connection is automated and involuntary from the point-of-view of the user of the network-enabled device, the user will not ordinarily be aware of the IP Address that the host network has assigned for his device. (www.webopedia.com/TERM/D/DHCP.html).

A portable device (laptops, tablets and smartphones) can make several different Internet connections through different host networks in any given day, depending on the desire of the user to move the portable device from place to place and to connect to the Internet. The bundles of data that constitute an Internet connection must have the source ID Address to function, so

[3] This article not only describes the process of "announcing" but also explains how the process can go wrong.

each Internet connection through a different network at a different location will have a different IP Address. Again, the process of exchanging the information that includes a different IP Address is ordinarily automated and involuntary from the point-of-view of the user of the portable device. (www.linktionary.com/d/dhcp.html).

These concepts can be tested with any laptop. If one were to log on to the Internet at home and open the website www.whatismyipaddress.com, for example, one would see the numerical IP Address that the laptop is showing to the Internet. That website will also provide the ISP and location information. If one were to then take the laptop to a coffee shop or restaurant and open whatismyipaddress.com, one would see that the laptop is showing a completely different IP Address to the Internet.

The process by which the website, whatismyipaddress.com, can identify the IP Address of a laptop visiting the website is relatively trivial. The host computer for a given website registers the IP Addresses of visitors that connect to it at any given time. (www.auditmypc.-com/ip-address.asp). The developers of whatismyaddress.com simply programmed the website to display the IP Address that the host computer had already registered.

Many host computers of websites maintain logs that list the IP Address of visitors along with date and time information. Websites that utilize a login feature (such as Twitter) can even maintain a log of IP Addresses and other data associated with the particular user who logged in. (twitter.com/privacy). If the user accesses the website with a portable device from different locations, then the user's data will include a variety of different IP Addresses.

The different IP Addresses will reflect the location and movement of the laptop and its owner. If, for example, one were to fly from Washington D.C. to Los Angeles and access the Internet at each stage of the journey, his laptop would adopt one IP Address for the wireless network at Dulles International Airport, a different IP Address in the air for accessing the Internet on a wifi-equipped airplane and a third IP Address for the destination hotel in Los Angeles.

If an analyst were provided with the three numerical IP Addresses for the networks at Dulles, on the airplane and at the Los Angeles hotel as well as the date-and-time-of-access

information and nothing else, then the analyst could readily put together the details of the journey using services available on the Internet. The "Whois" website permits a user to input a numerical IP Address and get the registry information of the ISP and location. Similarly, another service, MaxMind, is in the business of associating a given IP Address with physical address data that a person inputs into websites that he accesses and purports to give location information with greater precision. MaxMind is only one such service. Using those services, the three numerical IP Addresses would translate into locations for Washington D.C., the airline (although not the precise location of the plane at any given moment) and Los Angeles, thereby disclosing the broad details of the journey.

The Whois service can sometimes associate an IP Address with an exact location. For example, inputting the IP Address 156.128.118.200 into Whois shows that the Administrative Office of the Courts is located at One Columbus Circle NE, Washington D.C. On most other occasions, however, the Whois service will only associate an IP Address with a particular city or town.

Where that is the case, the problem of pinpointing a person's location and movements from a list of IP Addresses remains surmountable. The ISP will maintain records of the physical addresses associated with a given IP Address for a network within its system Once the government has a list of IP Addresses, it can subpoena subscriber information from the different ISPs for the specific IP Addresses and develop a detailed picture of a person's location and movements from that subscriber information. (www.nytimes.com/2008/04/05/opinion/-05sat4.html).

Even without ISP assistance, given a large amount of data about a person's IP Addresses, date-and-time of access information and nothing more, pinpointing location and movements simply presents a puzzle that some statistical analysis and a little fieldwork might be able to solve. Techniques associated with "statistical classification" or "pattern recognition" permit an unknown set of values to be derived from a known set of values. (en.wikipedia.org/wiki/Statistical_classification). Thus, if an analyst were given an IP Address known to be a target person's home, an IP Address known to be a target's office and an IP Address known to be a target's

favorite coffee shop, then statistical classification techniques could be used to identify a range of probable physical addresses for the other IP Addresses associated with the target. That range of physical addresses might then be further investigated in the field. If the puzzle were solved, then the end result would be a fairly accurate list of the target's locations and movements on different dates and times.

In addition, IP Address and date-and-time-of-access information can create an inference that two people were together in the same place at the same time. Suppose, for example, that two individuals logged in to Twitter at exactly the same date and time from a single IP Address associated with a Starbucks in Reykjavik, Iceland. That information would be highly suggestive of the fact that the two people were meeting each other.

IP Address information can also pierce anonymity online. A person might use his true name on one website and a pseudonym on the other. The IP Address information associated with the person's true name on the one website will correlate to the IP Addresses used with the pseudonym on the other website, thereby unmasking the person's identity.

Active users of the website, Twitter, potentially generate a great deal of data. Twitter is a web-based service on which a user can post short messages called "tweets." (support.twitter.-com/entries/15367-how-to-post-a-twitter-update-or-tweet). Active users can post many tweets during a given day, after having accessed the Internet with their portable devices at a variety of locations and through a variety of networks and after having logged into the Twitter website. Each network will cause Twitter to register a different IP Address and other data and associate that data with the user's login information. That large amount of data can then translate into a picture of the user's locations and movements, as described above.

Because an IP Address is associated with the network through which a portable device accesses the Internet, it is completely unlike a telephone number. A telephone number is either associated with a static address with respect to a land line or with a unique, portable device in the case of a cell phone. A land line telephone number cannot translate into tracking an owner from location to location because it does not move. A cell phone telephone number does not translate into the location and movement of its owner because the cell phone could be anywhere at the

time of a call. This is not to say that cell phones do not transmit location data to the telecommunications carrier; they do. However, under the reasoning set forth by the Third Circuit in *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010), the privacy interests associated with such information should compel the government to seek a warrant to gain access to that information.

In this matter, the government has obtained an order requiring Twitter to turn over IP Addresses and related data associated with the Parties over a six-and-a-half month period of time. Given the Parties' extensive use of Twitter, that is likely to encompass a very large amount of data about the Parties. As the foregoing demonstrates, the government can compose a picture of the Parties' locations and movements from that data over that extensive period of time.

One would assume that is the government's purpose for seeking the order in the first place.

IV. CONCLUSION

In summary, given the technology surrounding IP Addresses and the potential information that can be gleaned from them, the Parties' position that IP Addresses are more closely analogous to cell phone location information than to simple telephone numbers is correct. In addition, the Parties' assertion that this information can be used to track the physical location of users, including into traditionally constitutionally protected spaces, is also correct.

ATTORNEYS FOR AMICI CURIAE STEVEN M. BELLOVIN, PHD.
By Counsel

/S/_________________________
Thomas E. Moore III (*pro hac vice* pending)
The Moore Law Team
228 Hamilton Avenue/3rd floor
Palo Alto, CA 94301
(650) 789-5354
fax: (650) 789-5001
email: tmoore@moorelawtem.com

/S/_________________________
Marvin D. Miller
VSB #1101
Law Offices of Marvin D. Miller
1203 Duke Street
Alexandria, VA 22314
(703) 548-5000
fax: (703) 739-0179
email: katherine@marvinmilleratlaw.com

CERTIFICATE OF SERVICE

I hereby certify that on the 31st day of March, 2011, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system, which will then send a notification of such filing (NEF) to the following:

Tracy Doherty McCormick: tracy.mccormick@usdoj.gov, usavae.alx.ecf.frcc@usdoj.cov, usavae.alx.ect.nar@usdoj.gov

John K. Zwerling: jz@zwerling.com

Stuart Alexander Sears: stuart@zwerling.com

Nina J. Ginsberg: nginsberg@dimuro.com, ssingletary@dimuro.com

Jonathan Shapiro: js@greenspunlaw.com

Rebecca K. Glenberg: rglenberg@acluva.org

John K. Roche: jroche@perkinscoie.com

________/S/______________
MARVIN D. MILLER
V.S.B. No. 1101
Counsel for ____________________
Law Offices of Marvin D. Miller
1203 Duke Street
Alexandria, VA 22314
Phone: (703) 548-5000
Fax: (703) 739-0179
katherine@marvinmilleratlaw.com